



US009471920B2

(12) **United States Patent**
Kolkowitz et al.

(10) **Patent No.:** **US 9,471,920 B2**
(45) **Date of Patent:** **Oct. 18, 2016**

(54) **TRANSACTION ASSESSMENT AND/OR AUTHENTICATION**

(75) Inventors: **Dan Kolkowitz**, Los Altos Hills, CA (US); **Taher Elgamal**, Atherton, CA (US); **Kieran Gerard Sherlock**, Palo Alto, CA (US)

(73) Assignee: **IDM Global, INC.**, Palo Alto, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 584 days.

(21) Appl. No.: **12/776,784**

(22) Filed: **May 10, 2010**

(65) **Prior Publication Data**

US 2010/0293094 A1 Nov. 18, 2010

Related U.S. Application Data

(60) Provisional application No. 61/178,753, filed on May 15, 2009.

(51) **Int. Cl.**
G06Q 20/40 (2012.01)

(52) **U.S. Cl.**
CPC **G06Q 20/4016** (2013.01); **G06Q 20/40** (2013.01); **G06Q 20/4014** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/4016
USPC 705/39
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,963,915 A 10/1999 Kirsch
6,021,397 A 2/2000 Jones et al.

6,047,268 A	4/2000	Bartoli et al.
6,076,068 A	6/2000	DeLapa et al.
6,336,099 B1	1/2002	Barnett et al.
6,351,812 B1	2/2002	Datar et al.
6,571,339 B1	5/2003	Danneels et al.
6,691,915 B1	2/2004	Thaxton et al.
6,862,575 B1	3/2005	Anttila et al.
6,954,732 B1	10/2005	DeLapa et al.
7,290,278 B2	10/2007	Cahill et al.
7,356,507 B2	4/2008	Bezos et al.
8,639,629 B1	1/2014	Hoffman
2001/0024785 A1	9/2001	Keinath et al.
2002/0059130 A1	5/2002	Cheng et al.
2002/0099649 A1 *	7/2002	Lee et al. 705/38
2003/0149603 A1	8/2003	Ferguson et al.
2003/0163691 A1	8/2003	Johnson
2003/0187759 A1	10/2003	Arthus et al.

(Continued)

OTHER PUBLICATIONS

Fabian Monroe and Aviel D. Rubin, *Keystroke Dynamics as a Biometric for Authentication*, Mar. 1, 1999, 15 pages.

(Continued)

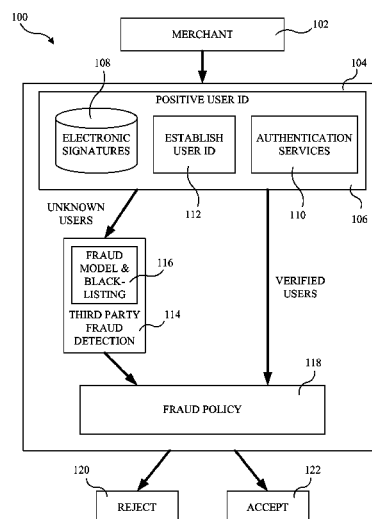
Primary Examiner — Eric T Wong

(74) *Attorney, Agent, or Firm* — Greenberg Traurig LLP

(57) **ABSTRACT**

Systems and methods for assessing and authenticating transactions are disclosed. Some exemplary embodiments may authenticate transactions based at least in part on a comparison of a newly obtained electronic signature associated with a user with a previously obtained electronic signature associated with the user, where a payment instrument presented for use in the transaction is also associated with the user. Exemplary electronic signatures may comprise any information which may identify the user, such as browser fingerprints, computer fingerprints, IP addresses, geographic IP location information, information associated with a payment, and/or a typing patterns.

7 Claims, 8 Drawing Sheets



(56)

References Cited

U.S. PATENT DOCUMENTS

2004/0010472	A1	1/2004	Hilby et al.	
2004/0117302	A1	6/2004	Weichert et al.	
2005/0278542	A1	12/2005	Pierson et al.	
2006/0031116	A1	2/2006	Bogasky et al.	
2006/0184428	A1	8/2006	Sines et al.	
2006/0282660	A1 *	12/2006	Varghese	G06Q 20/341 713/155
2007/0022058	A1	1/2007	Labrou et al.	
2007/0220595	A1 *	9/2007	M'raihi et al.	726/5
2008/0010678	A1	1/2008	Burdette et al.	
2008/0046334	A1 *	2/2008	Lee et al.	705/26
2008/0077515	A1	3/2008	Zoldi et al.	
2008/0140576	A1	6/2008	Lewis et al.	
2009/0048953	A1	2/2009	Hazel et al.	
2009/0089869	A1 *	4/2009	Varghese	726/7
2010/0094765	A1	4/2010	Nandy	
2010/0228580	A1	9/2010	Zoldi et al.	

2011/0251951	A1	10/2011	Kolkowitz et al.
2015/0081549	A1	3/2015	Kimberg et al.
2015/0220928	A1	8/2015	Allen
2015/0287026	A1	10/2015	Yang
2015/0310424	A1	10/2015	Myers
2015/0324802	A1	11/2015	Kolkowitz et al.
2015/0332256	A1	11/2015	Minor
2015/0363876	A1	12/2015	Ronca
2016/0063500	A1	3/2016	Sherlock et al.
2016/0071108	A1	3/2016	Caldera et al.

OTHER PUBLICATIONS

Non-final Office action, from U.S. Appl. No. 14/801,086, filed Jul. 16, 2015, mailed on Nov. 5, 2015, 17 pages, United States Patent & Trademark Office, Virginia, US.

Fighting Fraud in today's Connected World, Entrust Jul. 2009.

* cited by examiner

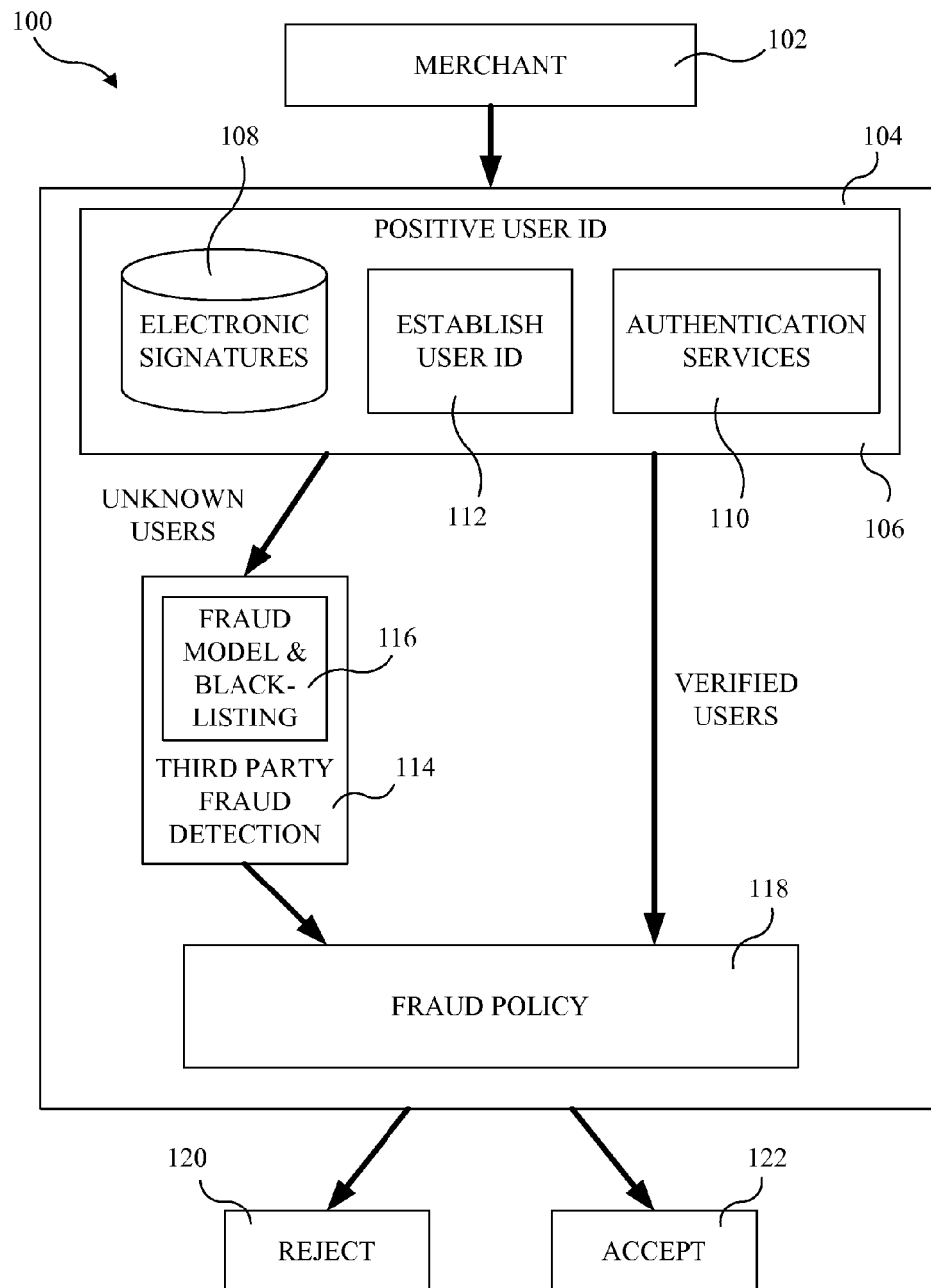


FIG. 1

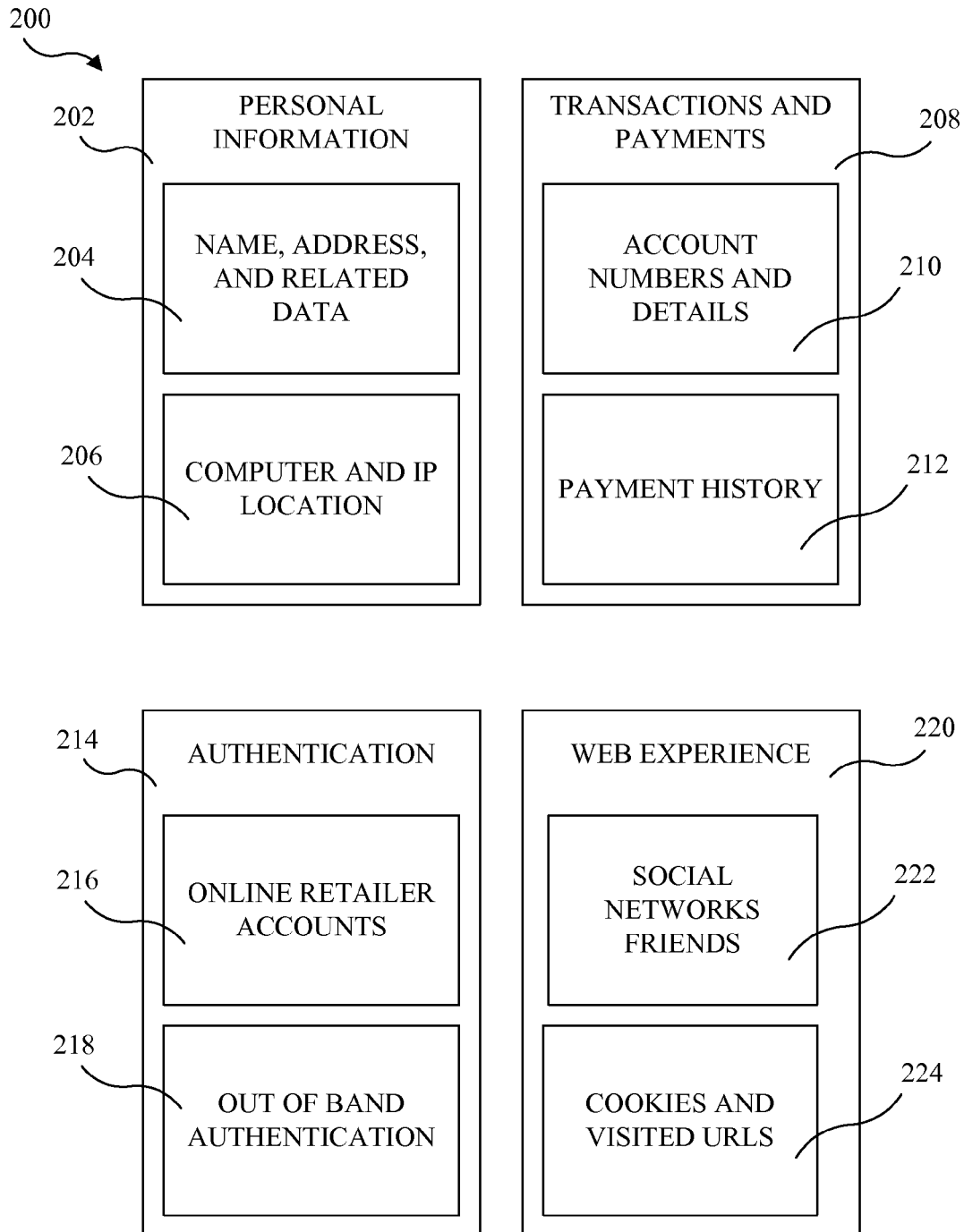


FIG. 2

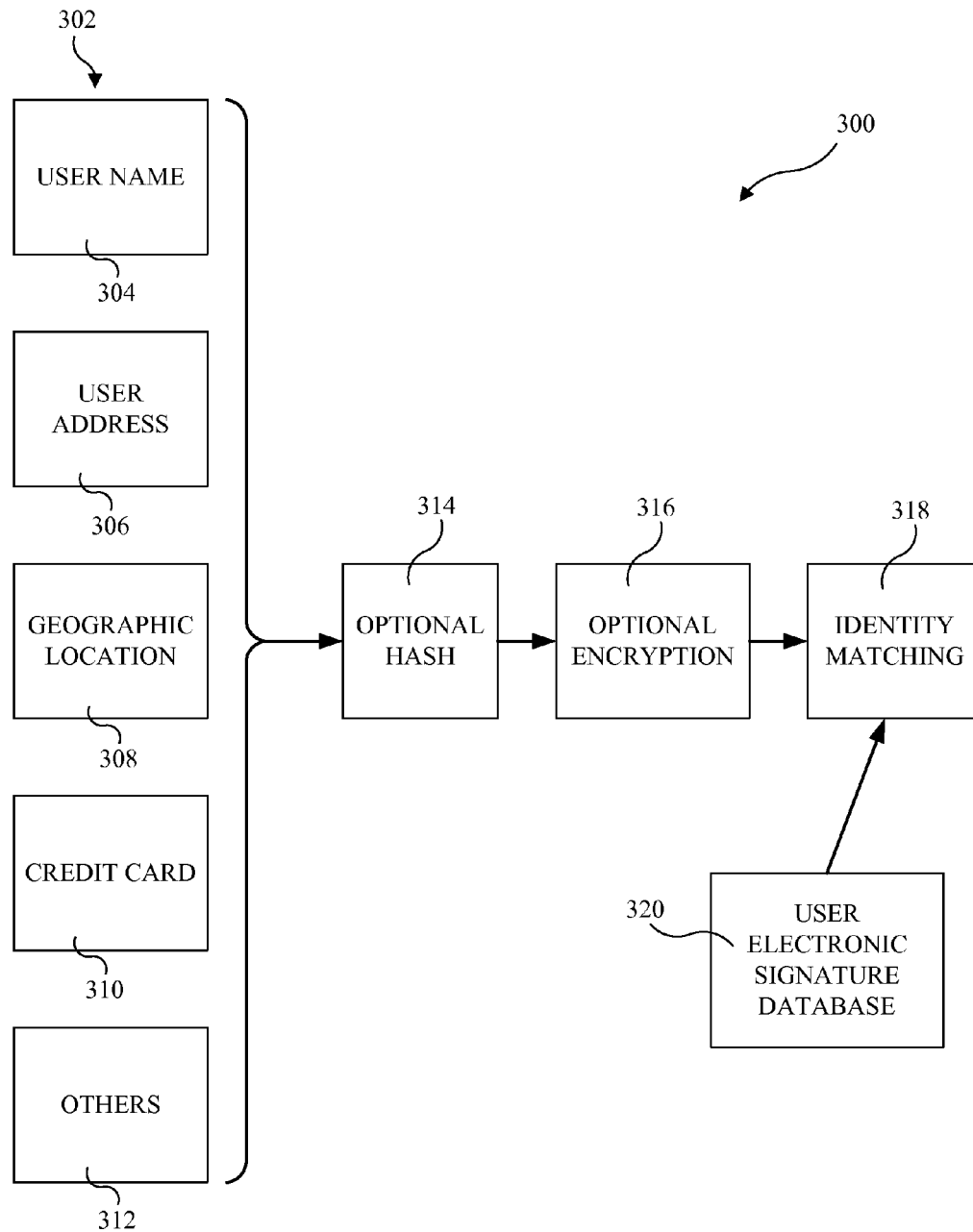


FIG. 3

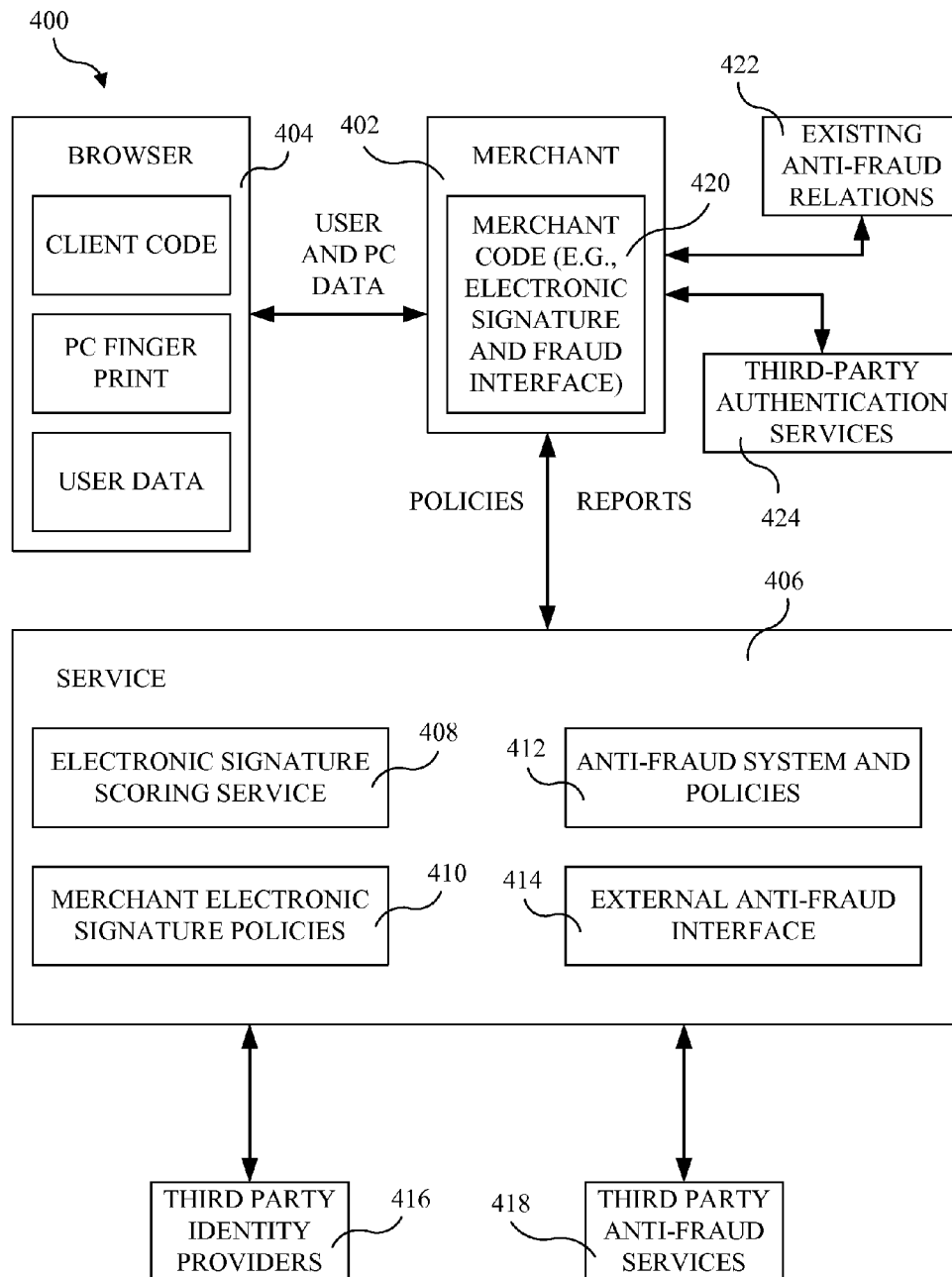


FIG. 4

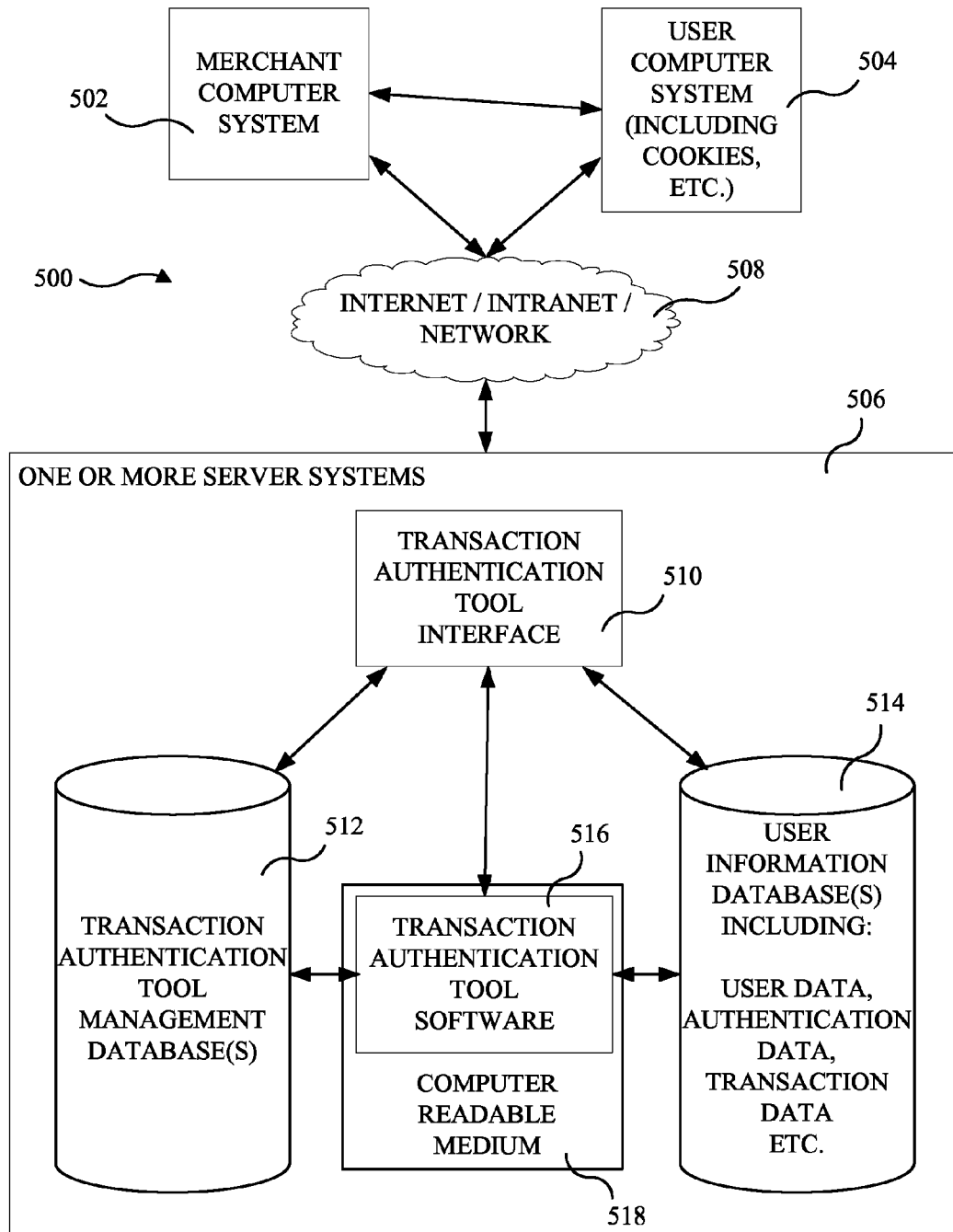


FIG. 5

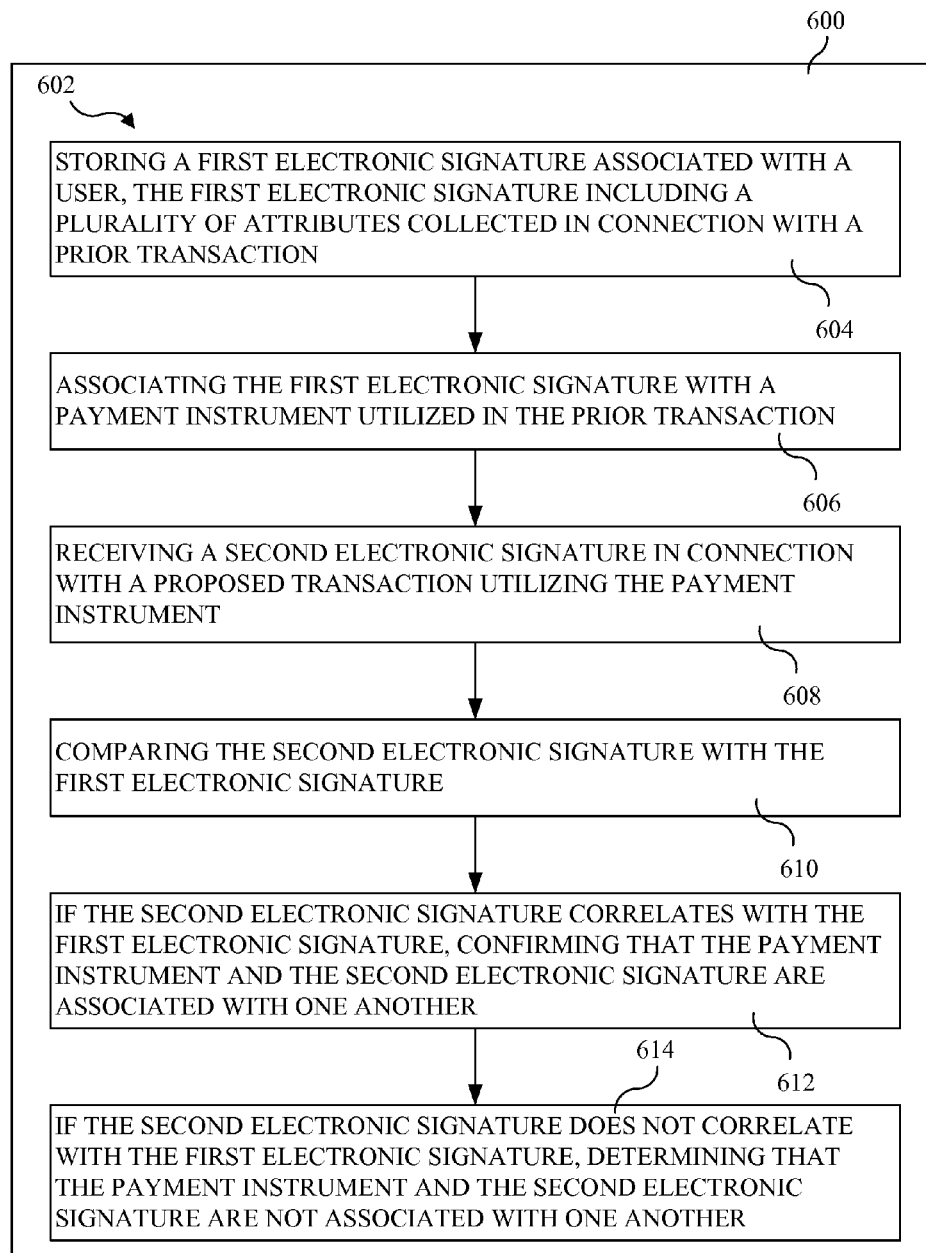


FIG. 6

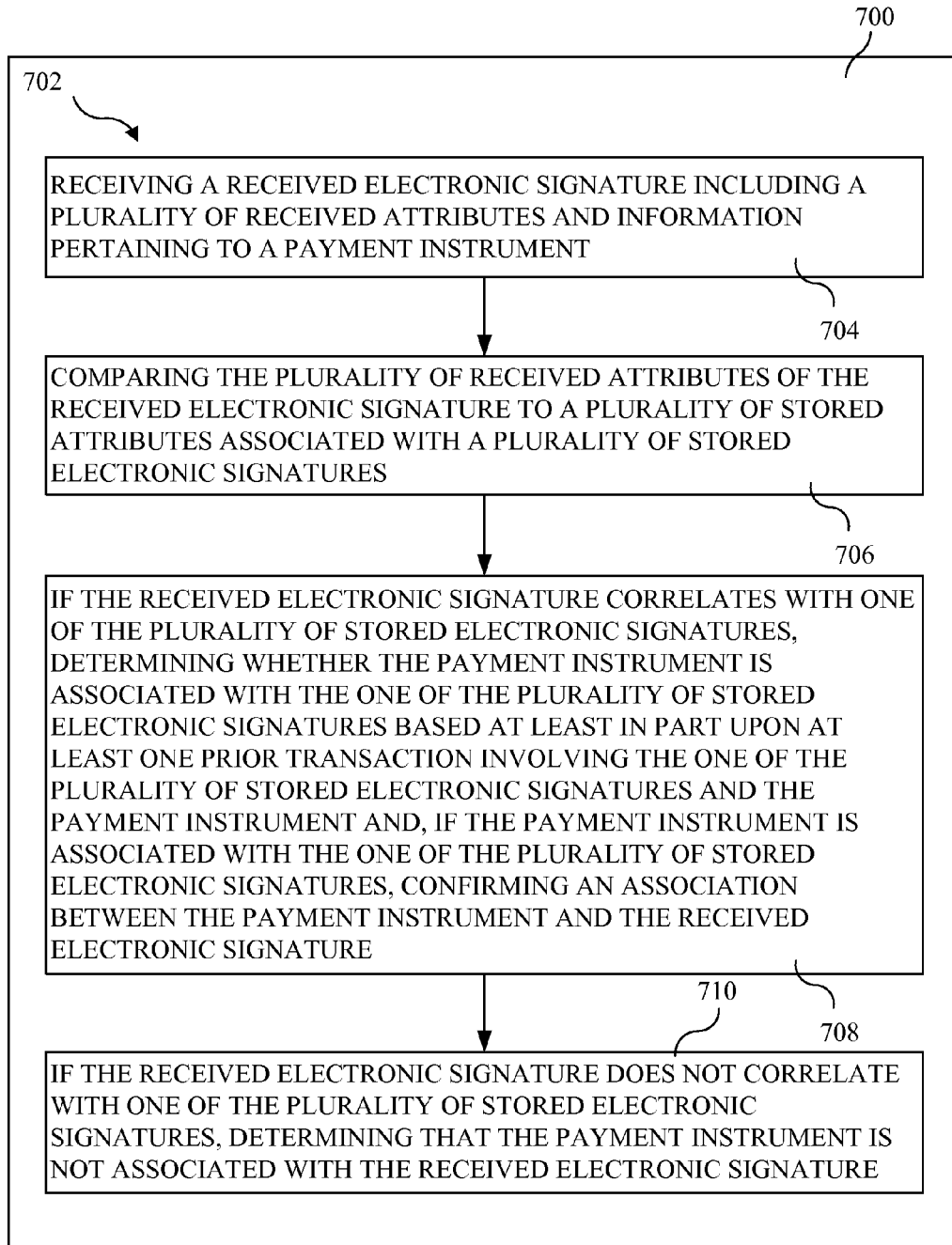


FIG. 7

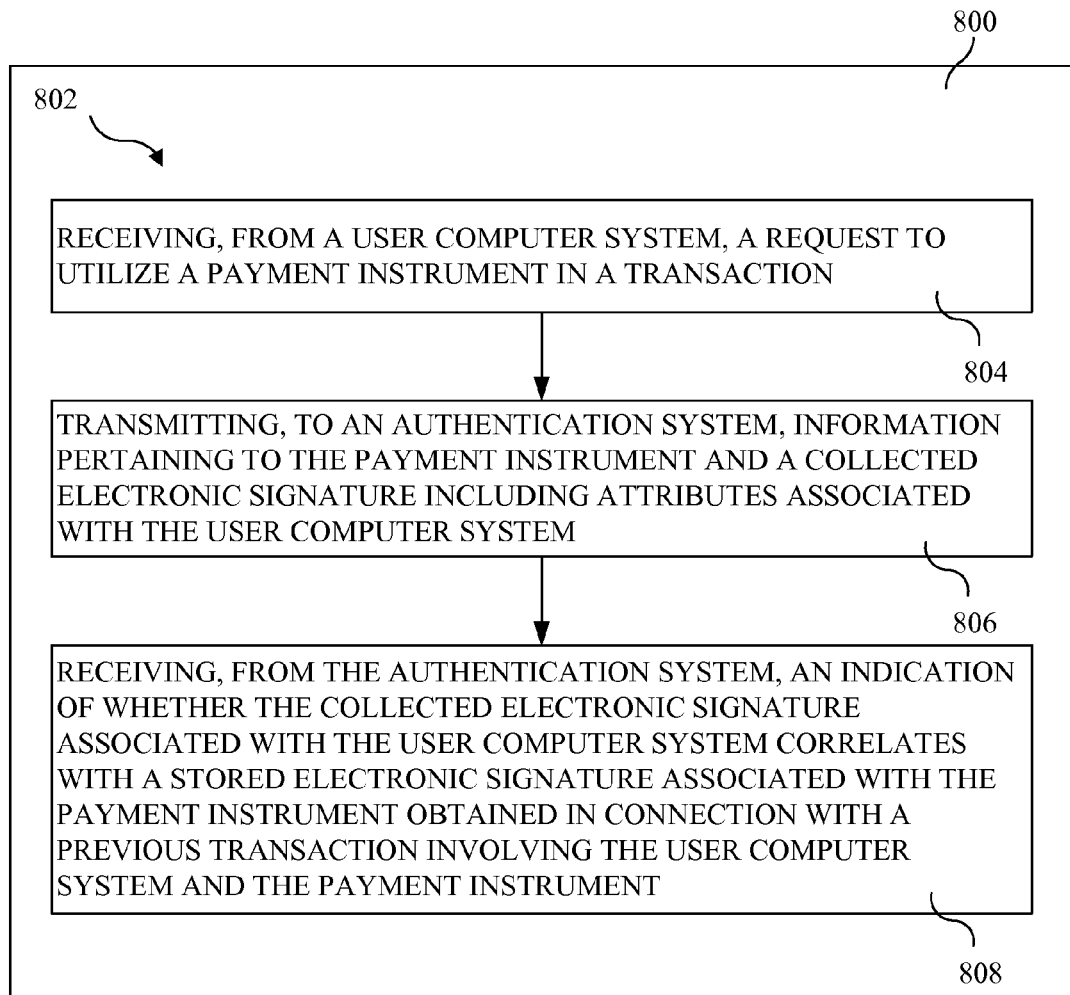


FIG. 8

1

TRANSACTION ASSESSMENT AND/OR AUTHENTICATION

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 61/178,753, filed May 15, 2009, which is incorporated by reference.

BACKGROUND

The present disclosure is directed to transaction assessment and/or authentication systems and methods and, more particularly, to systems and methods for assessing and/or authenticating transactions to identify fraudulent payments.

SUMMARY

Exemplary embodiments may include systems and methods for assessing and authenticating transactions are disclosed. Some exemplary embodiments may authenticate transactions based at least in part on a comparison of a newly obtained electronic signature associated with a user with a previously obtained electronic signature associated with the user, where a payment instrument presented for use in the transaction is also associated with the user. Exemplary electronic signatures may comprise any information which may identify the user, such as browser fingerprints, computer fingerprints, IP addresses, geographic IP location information, information associated with a payment, and/or a typing patterns.

In an aspect, an exemplary system may uniquely identify a user using the network and payment attributes presented in the regular contexts of payment transactions. Attributes may include browser fingerprints, computer fingerprints, IP addresses, geo-IP location information, information entered regularly on payment, the typing pattern when entering fields in the payment information. Such information may comprise an electronic signature and may uniquely identify a user across merchants and payment networks. In some exemplary embodiments, only when enough information is available to identify the user is the user known through his or her electronic signature.

In an aspect, an exemplary system may positively recognize a user through his or her payment and/or network behavior to approve transactions on the basis of being the known good user of a payment instrument.

In an aspect, an exemplary method may include collecting the history data of charges, entered information, and summary data on those transactions being accepted or rejected to build a database that becomes part of an electronic signature for a user.

In an aspect, an exemplary method may include using hashes of attributes collected in a transaction that can be stored at a central location and/or may be used in a positive system to uniquely identify known users to a collection of merchants and payment networks. The hashes may not be reversed to extract personal information, which may allow cooperation between merchants and payment entities without compromising customer information.

In an aspect, an exemplary method may include explicitly identifying a user on first use of a payment instrument for the purpose of collecting an electronic signature for use in subsequent network transactions.

In an aspect, an exemplary method may include a check of an electronic signature on a transaction for the purpose of

2

detecting whether the user is the same or not as a requirement for acceptance of a card-not-present transaction.

In an aspect, an exemplary method of detecting identity theft may include the use of an electronic signature to recognize the use of a card by a different user than the one to whom it was issued.

In an aspect, an exemplary method may include using a payment through a known trusted source as establishing a base reputation for a user with an electronic signature for a merchant or a collection of merchants not affiliated with the trusted source. For example, verification made through a trusted online retailer may be used to establish that the user was recognized and able to pay through those services, and may give an increased level of confidence that the user is known accurately to the service.

In an aspect, a computer-readable medium may computer-executable instructions stored thereon, which, when executed by a computer, enable the computer to perform a method including storing a first electronic signature associated with a user, the first electronic signature including a plurality of attributes collected in connection with a prior transaction; associating the first electronic signature with a payment instrument utilized in the prior transaction; receiving a second electronic signature in connection with a proposed transaction utilizing the payment instrument; determining whether the second electronic signature correlates with the first electronic signature by comparing the second electronic signature with the first electronic signature; if the second electronic signature correlates with the first electronic signature, confirming that the payment instrument and the second electronic signature are associated with one another; and if the second electronic signature does not correlate with the first electronic signature, determining that the payment instrument and the second electronic signature are not associated with one another.

In detailed embodiment, the plurality of attributes may include at least one of a browser fingerprint, a computer fingerprint, an IP address, geographic IP location information, information associated with a payment, a typing pattern, user name, user billing address, user shipping address, user phone number, email address, and account name. In a detailed embodiment, comparing the second electronic signature with the first electronic signature may include comparing individual attributes collected in connection with the proposed transaction to corresponding ones of the plurality of attributes collected in connection with the prior transaction. In a detailed embodiment, determining whether the second electronic signature correlates with the first electronic signature may be based at least in part upon a trust score calculated using a weighted consideration of at least some of the plurality of attributes collected in connection with the prior transaction. In a detailed embodiment, the weighted consideration may include calculating the trust score based at least in part upon matching attributes, non-matching attributes, attributes not compared, and a maximum possible trust score.

In a detailed embodiment, determining whether the second electronic signature correlates with the first electronic signature may include calculating a trust score based at least in part upon at least one of a reputation score associated with the payment instrument, a reputation score associated with a computer utilized in the proposed transaction, and a reputation score associated with the user.

In a detailed embodiment, the browser fingerprint may include at least one of a user agent, a screen resolution, a software plug-in, a time zone, a system language, whether Java is enabled, whether cookies are enabled, a site visited,

3

and an IP address. In a detailed embodiment, the computer fingerprint may include at least one of a processor characteristic, a memory size of the machine, a value that is loaded at a key location, a value of a registry of a loaded operating system, an Ethernet MAC address, raw networking information, network information, a loaded program, and a log file. In a detailed embodiment, the network information may include a network provider, whether an IP address is consistent with a known IP address, a geographical proximity of an address registered with a payment instrument and the IP address as determined by an IP to geo-location service, whether or not a proxy is in use, whether a known bad IP address is in use, and whether the IP address is associated with a service provider who was associated with the user in the prior transaction.

In an aspect, a computer-readable medium may include computer-executable instructions stored thereon, which, when executed by a computer, enable the computer to perform a method including receiving a received electronic signature including a plurality of received attributes and information pertaining to a payment instrument; determining whether the received electronic signature correlates with any of a plurality of stored electronic signatures by comparing the plurality of received attributes of the received electronic signature to a plurality of stored attributes associated with the plurality of stored electronic signatures; if the received electronic signature correlates with one of the plurality of stored electronic signatures, determining whether the payment instrument is associated with the one of the plurality of stored electronic signatures based at least in part upon at least one prior transaction involving the one of the plurality of stored electronic signatures and the payment instrument and if the payment instrument is associated with the one of the plurality of stored electronic signatures, confirming an association between the payment instrument and the received electronic signature; and if the received electronic signature does not correlate with one of the plurality of stored electronic signatures, determining that the payment instrument is not associated with the received electronic signature.

In a detailed embodiment, the information pertaining to the payment instrument may include a credit card number.

In a detailed embodiment, the plurality of received attributes may include at least one of a browser fingerprint, a computer fingerprint, an IP address, geographic IP location information, information associated with a payment, a typing pattern, user name, user billing address, user shipping address, user phone number, email address, and account name. In a detailed embodiment, the browser fingerprint may include at least one of a user agent, a screen resolution, a software plug-in, a time zone, a system language, whether Java is enabled, whether cookies are enabled, a site visited, and an IP address. In a detailed embodiment, the computer fingerprint may include at least one of a processor characteristic, a memory size of the machine, a value that is loaded at a key location, a value of a registry of a loaded operating system, an Ethernet MAC address, raw networking information, network information, a loaded program, and a log file. In a detailed embodiment, the network information may include a network provider, whether an IP address is consistent with a known IP address, a geographical proximity of an address registered with a payment instrument and the IP address as determined by an IP to geo-location service, whether or not a proxy is in use, whether a known bad IP address is in use, and whether the IP address is associated with a service provider who was associated with the user in the prior transaction.

4

In a detailed embodiment, determining whether the received electronic signature correlates with any of the plurality of stored electronic signatures may include determining which ones of the plurality of received attributes match stored attributes associated with individual stored electronic signatures. In a detailed embodiment, determining whether the received electronic signature correlates with any of the plurality of stored electronic signatures may include calculating a trust score based at least in part upon which ones of the plurality of received attributes match stored attributes associated with individual stored electronic signatures. In a detailed embodiment, calculating the trust score may include applying different weights to different ones of the plurality of received attributes. In a detailed embodiment, calculating the trust score may be based at least in part upon a reputation score. In a detailed embodiment, the method may include, if the trust score is below a first predetermined threshold, determining that the payment instrument is not associated with the received electronic signature; if the trust score is between the first predetermined threshold and a second predetermined threshold, determining that the payment instrument is associated with the received electronic signature at a low confidence level; and if the trust score is above the second predetermined threshold, determining that the payment instrument is associated with the received electronic signature at a high confidence level.

In an aspect, a computer-readable medium may include computer-executable instructions stored thereon, which, when executed by a computer, enable the computer to perform a method including receiving, from a user computer system, a request to utilize a payment instrument in a transaction; transmitting, to an authentication system, information pertaining to the payment instrument and a collected electronic signature including attributes associated with the user computer system; and receiving, from the authentication system, an indication of whether the collected electronic signature associated with the user computer system correlates with a stored electronic signature associated with the payment instrument obtained in connection with a previous transaction involving the user computer system and the payment instrument.

In a detailed embodiment, the attributes associated with the user computer system may include at least one of a browser fingerprint, a computer fingerprint, an IP address, geographic IP location information, information associated with a payment, a typing pattern, user name, user billing address, user shipping address, user phone number, email address, and account name.

In a detailed embodiment, the indication may include at least one of an indication corresponding to a high confidence correlation, a low confidence correlation, and no correlation. In a detailed embodiment, the method may include, if the indication corresponds to the high confidence correlation, accepting the transaction; if the indication corresponds to the low confidence correlation, initiating additional fraud detection assessment; and if the indication corresponds to no correlation, rejecting the transaction. In a detailed embodiment, the high confidence correlation may be associated with a high user match score, a known payment instrument, a known computer that have previously been used together.

BRIEF DESCRIPTION OF THE DRAWINGS

The detailed description refers to the following figures in which:

FIG. 1 is a block diagram illustrating an exemplary transaction assessment and authentication environment;

5

FIG. 2 is a block diagram illustrating example information which may be collected and/or utilized in electronic signatures;

FIG. 3 is flow chart illustrating an exemplary transaction assessment and authentication method;

FIG. 4 is block diagram illustrating an exemplary system for assessing and authenticating a transaction;

FIG. 5 is a block diagram illustrating an exemplary system for assessing and authenticating a transaction;

FIG. 6 is a block diagram illustrating an exemplary computer-readable medium;

FIG. 7 is a block diagram illustrating an exemplary computer-readable medium; and

FIG. 8 is a block diagram illustrating an exemplary computer-readable medium; all in accordance with at least some aspects of the present disclosure.

DETAILED DESCRIPTION

The illustrative embodiments described in the detailed description and drawings are not meant to be limiting. Other embodiments may be utilized, and other changes may be made, without departing from the spirit or scope of the subject matter presented here. It will be readily understood that the aspects of the present disclosure, as generally described herein, and illustrated in the figures, may be arranged, substituted, combined, and designed in a wide variety of different configurations, all of which are explicitly contemplated and make part of this disclosure.

The present disclosure relates, inter alia, to methods and systems associated with transaction assessment and/or authentication and, more particularly, to assessing and/or authenticating transactions to identify fraudulent payments.

The present disclosure contemplates that transaction fraud is becoming more prevalent due, in large part, to the Internet. For example, transaction frauds may include fraudulent use of payment instruments such as credit cards, debit cards and other similar instruments. Some fraud-check systems maintain lists of known bad cards, bad addresses, and/or bad computer system fingerprints, which may be referred to as "black lists." Further, some fraud-check systems perform analytics with the bad cards, bad addresses, and/or bad computer system fingerprints to determine whether a given transaction appears legitimate. Some of these fraud-check systems also determine a risk associated with a transaction.

Some exemplary embodiments according to the present disclosure may utilize information associated with a user to develop and/or maintain an association between a user and a payment instrument. In some exemplary embodiments, transaction assessment and/or authentication systems and methods may be configured to collect information associated with a user of a payment instrument and/or to compare such newly collected information with previously collected information. Based at least in part upon the comparison of the previously collected information and the newly collected information, some exemplary systems and methods may be configured to determine whether the user is associated with the presented payment instrument. Some exemplary embodiments may be configured to maintain all or part of the information related to users' transactions over time, which may increase the level of trust in an identity matching scheme.

Some exemplary embodiments may utilize data that may be collected in transactions using Internet online payment systems for online merchants. For example, data associated with a transaction may be collected to build a representation of the user who is associated with the payment instrument

6

used in the transaction. In some exemplary embodiments, data associated with attributes that can be seen in the network and/or the transaction that may be associated with and/or may identify a user may be analyzed and/or used to create an electronic signature of the user. Exemplary attributes include, but are not limited to, browser fingerprints, computer fingerprints, IP addresses, geographic IP location information, information associated with a payment, and/or a typing pattern when entering data in fields related to the payment. Browser fingerprints may include attributes associated with an individual's browser that may be extracted using standard interfaces. For example, browser fingerprints may include characteristics such as user agent (includes browser and operating system), screen resolution, software plug-ins (in a manageable state), time zone, system language, whether Java is enabled, whether cookies are enabled, sites visited, and/or IP address. The present disclosure contemplates that matching browser fingerprint characteristics in a subsequent interaction with those collected during a prior interaction may indicate a high probability that the same browser was used in both the prior and subsequent interactions.

Some exemplary computer fingerprints may allow a determine of whether a physical machine is the same as one that has been seen in the past. Computer fingerprints may include, for example, processor characteristics (e.g., model number, version, speed, cache size serial number, etc.), memory size of the machine, values that are loaded at key locations, values of the registry of the loaded operating system, Ethernet MAC (media access control) address, raw networking and network information (e.g., configuration parameters), loaded programs, and/or log files. Some exemplary embodiments may utilize performance on specified benchmark program fragments, such as by measuring the performance of a program that includes different characteristics including input/output and CPU (central processing unit) speed. Such an approach may take into account the other processes running on a user's machine, the amount of memory, etc., and it may provide reproducible results so that it may act as a part of a fingerprint. Example information associated with a payment may include behaviors observed on entered information (e.g., typing rhythms, billing addresses entered, cards used, passwords or PINs stored and/or requested), Zip code, full name entered, and/or loaded verses empty fields on entering information (for example, the browser may have the previously entered values from the last instance of the user). This can be seen to be entered by the browser rather than typing by the speed of entry of the characters. In some exemplary embodiments, the electronic signature may uniquely identify the user at the same merchant in future transactions and/or at other merchants where the same attributes can be seen.

In some exemplary embodiments, when a transaction is presented by a user to a merchant, data related to the user's electronic signature may be collected. The newly collected electronic signature data may be compared to previously collected electronic signature data associated with that user to determine whether or not the newly collected electronic signature correlates with the previously collected electronic signature. If the newly collected electronic signature correlates with the previously collected electronic signature, then it may be assumed that the user has been identified. If the newly collected electronic signature does not correlate with the previously collected electronic signature, then it may be assumed that the user in the present transaction is not the same user who participated in previous transactions. Thus, by associating a particular payment instrument with a known

7

user (e.g., by identifying the user by his or her electronic signature), it may be determined whether or not the payment instrument presented in a particular transaction is known to belong to the user who is presenting the payment instrument.

In some exemplary embodiments, a lack of correlation between the newly collected electronic signature and the previously collected electronic signature may be used to identify transactions which may merit further assessment. For example, if the newly collected electronic signature correlates with a known, previously collected electronic signature of a different user (e.g., a user other than the user involved in the transaction), then the transaction may be flagged for further assessment, such as further determination of whether or not fraud is involved or whether additional fraud checks need to be performed.

The present disclosure contemplates that the notion of using an electronic signature associated with a user to identify the user in a payment network may be aided by the standardization of World Wide Web interfaces. Merchant payment interfaces often utilize standard World Wide Web technology to provide user catalogs and payment collection. This may include the input of credit card and/or other payment information through applications running on users' computers or as browser applications. Some exemplary embodiments according to the present disclosure may be configured to collect certain pieces of information for the purpose of identifying the user who is behind the payment instrument. Some of these pieces of information are not necessarily related to the transaction, but may instead relate to characteristics of the user's computer environment and/or network sessions. For example, characteristics of the user's computer environment may include browser fingerprint information and/or typing characteristics of the user. Characteristics of the network sessions may include IP address, whether or not the user is coming from a known location associated with the user, and/or whether or not the user is utilizing a network proxy. The whole collection of the information (or parts thereof) may provide a unique user electronic signature. Such an electronic signature may allow a determination of whether a particular user is associated with a particular payment instrument they are presenting.

As illustrated in FIG. 1, an exemplary transaction assessment and authentication environment 100 may include a merchant 102 submitting information pertaining to a transaction to a transaction assessment and authentication system 104. System 104 may include a positive user ID module 106, which may employ an electronic signature database 108 and/or authentication services 110 to establish a user ID 112. Users who are not positively identified (e.g., unknown users) may be subjected to one or more third party fraud detection processes 114, such as fraud model and/or black listing analyses 116. Users who are positively identified (e.g., verified users) and/or unknown users who have undergone third party fraud detection processes 114 may be evaluated under a fraud policy 118, and system 104 may provide an accept 120 or reject 122 output associated with the user.

FIG. 2 illustrates example information 200 which may be collected and/or utilized in electronic signatures. Personal information 202 may include a user's name, address, and related information 204 and/or computer and IP location information 206. Transactions and payments information 208 may include account numbers and details 210 and/or payment history information 212. Authentication information 214 may include information associated with online retailer accounts 216 and/or out of band authentication 218 (e.g., authentication of the user via communications channels other than the primary communications channel being

8

used to conduct the transaction, such as authentication using a telephone for a transaction conducted via the internet). Web experience information 220 may include social networks friends 222 and/or website-related data 224, such as cookies and/or visited URLs (uniform resource locators) associated with the user's web experience.

Some exemplary embodiments may be configured to utilize electronic signatures to identify users, or as a common component in the identification of users. In some exemplary embodiments, this may reduce or eliminate dependence upon user-supplied information to identify users. In some exemplary embodiments, the actual underlying data in an electronic signature may be less important than correlation between aspects of a newly collected electronic signature and a previously collected electronic signature.

Some exemplary embodiments may reduce the likelihood that a user's identity may be hidden. For example, some exemplary embodiments may assess the degree of correlation of a newly collected electronic signature with a previously collected electronic signature. The degree of correlation may be evaluated to determine whether such electronic signatures uniquely identify the user. If so, the electronic signature may be considered to be positive identification of the user in the transaction.

Some exemplary embodiments may use any technology to help identify a user at their computer or site using identifying attributes and/or data. Instead of (or in addition to) using technologies to generate "blacklists" (or negative lists of users with bad payment credentials), some exemplary embodiment may use attributes to help identify the user in different contexts. The present disclosure contemplates that the attributes may not necessarily identify the user completely. Cryptographic techniques may be used to store encrypted information that may be transmitted by the user. The encrypted information may assist a merchant in determining the identification of a consumer (user) using a payment instrument.

As illustrated in FIG. 3, some exemplary transaction assessment and authentication methods 300 may include cryptographic hashing and/or encryption of the information. For example, newly collected electronic signature information 302, such as user name 304, user address 306, geographic location 308, credit card data 310, and/or other information 312, may be run through a hash operation 314 and/or encryption operation 316 prior to conducting identity matching 318 to evaluate the correlation with a previously collected electronic signature, such as from an electronic signature database 320. In some exemplary embodiments, the original information run through the hash and/or encryption operations may not be readily obtained from the hashed and/or encrypted result. In such embodiments, the correlation of the newly collected electronic signature and the previously collected electronic signature may be performed on hashed and/or encrypted data. Thus, although the actual information making up the electronic signature may not be retrievable (e.g., only hashed and/or encrypted data may be transmitted), assessment of correlation (e.g., matching) of attributes may be performed. For example, while the geographic location of a user may not be retrievable from the hash of the geographic location data, the newly obtained hash of the user's geographic location may be compared to a previously collected hash of the user's geographic location. If the hashes match, then the newly collected and previously collected geographic locations correlate.

In some exemplary embodiments, using hashed and/or encrypted data may allow private user data to be transmitted

across the internet only in hashed and/or encrypted form, which may provide privacy advantages. In some exemplary embodiments, using hashed and/or encrypted data may allow a plurality of merchants or other parties to cooperate to reduce fraudulent transaction without divulging confidential customer information. For example, merchants or other parties may contribute hashed and/or encrypted information comprising user electronic signatures which may be used by other parties for transaction assessment through matching. However, because the information is hashed and/or encrypted, the underlying information may not be retrievable.

Some exemplary embodiments may determine whether a payment instrument belongs to a user based on network information associated with the user. For example, network information associated with the user may include the network provider, whether the IP address is consistent with the user's known IP address, the geographical proximity of the address registered with a payment instrument (e.g., credit card or payment card) and the IP address as determined by an IP to geo-location service, whether or not the user is utilizing a proxy or known bad set of IP locations as determined by a service or black list, and/or whether the IP address is associated with a service provider who was associated with the user in past transactions. In this manner, some exemplary embodiments may enable a merchant to accurately assess whether a payment instrument (such as a credit card) belongs to the user of the payment instrument or not.

Some exemplary embodiments may address a growing problem with on-line and/or Internet transaction payments. For example, when a merchant receives a user request to charge a credit card, it may be beneficial to determine whether to accept the request based on the information presented by the user. In the case of stolen credit cards, the information about the user may be stolen at the same time along with the physical and/or virtual credit card information. This information may include a name, address, phone number and other pieces of billing and/or personally identifiable information. Since each merchant may verify their own customer's data, the personal data utilized for this kind of fraudulent activity may be replicated over and over. Some exemplary embodiments may reduce problems associated with the loss of that information and verification by the merchant. For example, if the system detects that a different user is using a known payment instrument, it may alert certain parties of the possibility of identity theft. By establishing the user's identity prior to processing the transaction, some exemplary embodiments may allow Internet payments to approach card-present situations in terms of fraud prevention and trustworthiness.

In some exemplary embodiments, the systems and methods described herein may assist merchants in determining whether they should accept a credit card payment based on whether the user making the payment owns the credit card. This may provide confidence and/or information to the merchant that the user owns the credit card. Such information may be considered by the merchant before processing the credit card payment. Some exemplary embodiments may reduce the differences between transactions where the credit card is present ("card-present" transaction) and transactions where the credit is not present ("card not present" transactions) since it may help establish that the user actually owns the credit card in an analogous way to clerk asking a person for drivers license and/or other credentials by matching the name and/or other information on the credit card with the license information. This may be a useful tool for all

involved parties since it tends to provide proof that a user owned the credit card, presented the credit card to the merchant and that the merchant performed the actual fraud checks. This may be better than in many "card-present" cases, as a merchant may not be able perform the required identity checks and there may be no record of whether they were performed.

Some exemplary embodiments may determine whether the payment requesting user is the same user who actually owns the card, instead of asking if a user's credentials are bad (e.g., whether they are on a blocked list, or are coming from known bad computer systems, etc.). This may be accomplished using much of the same data. But, the data may be transmitted to the authentication system to determine whether it is the same data that has been associated with the use of the card on an authentication network. In this manner, the authentication system may help determine whether it is the user that actually owns the payment instrument (as opposed to merely whether the transaction may be risky). This may provide much better user authentication than the explicit password-based authentication methods that are used in some systems today. Some exemplary embodiments may produce a trust level (or score) indicating how close the user requesting a current payment is to the known users of the card. A trust score may weight matching elements to provide a high score for matching of all elements and a very low or medium score for instances in which there are partially matching or non-matching elements.

In some exemplary embodiments, a trust score may be calculated as follows. A set of candidate users may be identified base on known existing good users of the payment instrument presented, known existing users of the computer from which the payment request is being made, users who have made purchases through the merchant account currently requesting payment, users sharing the same email address, and/or other criteria that find candidate users with a reasonable probability of matching the user requesting payment. For each of the candidate users, the attributes of the current payment request may be compared with the attributes of the candidate user to determine which candidate user, if any, is best matched by the current payment request. In some exemplary embodiments, the attributes may include user name, user billing address, user shipping address, user phone numbers (mobile, work, home, fax, etc.), user typing rhythms, email address, merchant account name. For purposes of matching, each of these attributes may be given a weight that reflects how strongly the presence of the attribute identifies the user. An exemplary table of user attribute weights follows:

Attribute	Weight (0-100)
User Name	10
User Billing Address	10
User Shipping Address	30
User Phone number	10
User Typing rhythm	50
User email address	20
User merchant account name	10

An overall match score may be calculated for each of the candidate users as follows. The weights of all of the attributes that matched may be summed and designated, "matchWeight." The weights of all of the attributes that did not match may be summed and designated "missWeight." The weights of all of the attributes of the candidate user may be summed and designated "maxPossible." The weights of all

11

of the attributes of the candidate user that were not present in the current payment request may be summed and designated "notInRequest."

In some exemplary embodiments, the match score may be given by the following expression:

$$\frac{(\text{matchWeight}^2 - (\text{missWeight} * 2) - \text{notInRequest}) * 1000}{\text{maxPossible}^2}$$

The best-matched user may be the candidate user with the highest match score.

In some exemplary embodiments, individual known cards, computers, and users within the authentication system may have individual reputation scores that may be determined by the history of payments involving that entity. For example, a user that has been involved in many successful transactions over a long period of time, none of which have been subsequently reversed due to fraud, may have a high reputation score. Similarly, a user that has been the subject of fraudulent transaction reversals (e.g., chargebacks) may have a low reputation score.

The trust score of the user that is requesting payment may be a function of the user match score, the reputation score of the user, payment instrument, and computer involved in the payment request, and/or the strength of any existing relationships between the payment instrument and computer.

The following exemplary algorithm illustrates how these inputs can be used to calculate a trust score for the payment requesting user:

1. If User match score is high AND payment instrument is known AND computer is known AND all have good reputations AND all have been used together THEN trust score=VERY GOOD
2. If user, payment instrument, or computer have a low reputation then trust score=BAD
3. If user match score low AND payment instrument is known AND computer is known AND all have good reputations AND all have been used together THEN trust score=GOOD
4. Otherwise trust score=SUSPICIOUS

A trust score may be used, for example, to determine how much scrutiny to apply to the transaction from a fraud analysis perspective. For example, if a user's trust score is VERY GOOD or GOOD then only limited resources may be applied to this user's transaction. Similarly if a user's trust score is BAD then the transaction may be rejected without further analysis. However if a user's trust score is SUSPICIOUS then this may be a transaction that deserves closer inspection.

In some exemplary embodiments, accumulating the transactions performed by users may improve the accuracy of these scores over time.

Some exemplary embodiments may reduce problems associated with stolen credit cards used on the Internet (e.g. when a user presents a credit card to a merchant, the merchant may ask if the user owns the credit card, and, if not, then merchant must perform more checks to determine if the credit card is stolen). If the user is known to the authentication system, then the merchant may know that the credit card is being used legitimately. If the user is not known to the authentication system, then the merchant may make a separate determination of the riskiness of the transaction (e.g., by checking black lists). Thus, some exemplary embodiments may reduce the frequency of checking the black lists in many cases, since most transactions are in fact legitimate.

In some exemplary embodiments, the authentication system may operate in a computer network environment as

12

follows. The merchant may embed a code in their applications which may take data from the user's environment and pass it across to the authentication system. For example, such data from the user's environment may include the same data as the browser fingerprint as described above. In the user's browser, an encrypted cookie may store any data that is passed to the authentication system. The encrypted cookie may also store user's information that has been previously known. In one embodiment, the user may not see the data, as it may only be a credential that gets transmitted to the authentication system. Some exemplary embodiments may compare the previous values with the values that are passed across in the active session. If an application operates outside of the browser, the routines may use the same protocol, but assemble their own cookie outside of the browser cookie facilities and cache.

Further, in some exemplary embodiments, a central server may receive requests from merchants. An application programming interface (API) may send the cookie together with the network information for the user. This may include all the components of the API which may be gathered by the embedded code. When the user presents the information to the authentication system through the API, they may include the cookie (which may include past behavior and/or local information). If information in the cookie does not match the current information, then a message may be provided that the user cannot be identified and/or authenticated. In such a case, a user may be identified by the authentication system by a number of different methods. The methods may lead to the same or similar corroborating information.

In some exemplary embodiments, transactions may occur with merchants, issuers and/or any entity that the user might want to present the payment instrument to. When a user presents a payment instrument to a merchant (for example), the merchant may request assistance from the authentication system to determine whether the user is the same user who has used the payment instrument in the past. In contacting the authentication system, the user may transmit data associated with the user's computer system and/or network connection (including an IP address, for example). The authentication system may utilize this data to make a determination as to whether the user is the same user who has used the same payment instrument in the past.

In some exemplary embodiments, the payment instrument issuer may set up a policy so that when a user presents the payment instrument, a check may be performed to confirm that the user's information matches the policy for the user identified as owning the payment instrument. Otherwise, the user may be deemed not authenticated.

In some exemplary embodiments, a merchant (for example) may collect data from the connection according to a policy that may be provided by the central authority. The user may not know what information to collect, nor may they give any information about themselves except network information that is being transmitted and information that may be gathered from the network connection. The authentication system may analyze whether the payment instrument information is coming from the user or another entity. If the merchant has implemented authentication system algorithms for identifying the user, then it may be determined with near certainty that it is the user. Otherwise, a result may be returned that indicates that positive identification of the user cannot be determined. Future transactions may then be known with relative certainty.

In some exemplary embodiments, a set of APIs may collect information related to the behavior of the user involved with the transaction. This may be deemed a "fin-

gerprint" of the user. The fingerprint may be used as part of the electronic signature of the user.

In some exemplary embodiments, when a merchant is asked to accept payment for a transaction, they may ask the authentication system whether this is the same user as defined by the issuer/authority for the payment instrument. The merchant may not make any determination of whether the payment should be taken. Instead, the authentication system may determine whether the user owns the payment instrument, and if the payment should be accepted. Based, at least in part, on the user's information (including network information, for example), the decision may be made whether this is the same user that owns this payment instrument as has been seen in the past on the Internet. If the user has registered with the payment instrument issuer, the determination of whether the user is the actual owner of the credential may be easily effectuated. The merchant may not know anything about the user beyond what they know through accepting the payment instrument. There is no identity of the user that is transmitted around the authentication system. Thus, some exemplary embodiments may maintain privacy of all users in the system while verifying their ownership of their payment credentials through matching their electronic signatures.

In some exemplary embodiments, a method to determine the identity of a user through use of network signatures may be provided. An exemplary network signature may include information known about the browser or computer environment, the IP address, networking locations that the user is known to come from, and/or the total history of the user's behavior. The network signature for a user may provide a unique identity in various contexts. This method may include weighing components of the network characteristics gathered through a user's activity on the Internet.

In some exemplary embodiments, the algorithm to calculate a trust score for a payment requesting user described above may be adapted to identify the user via their network characteristics by substituting attributes of the user's network signature for user attributes. An exemplary table of network characteristic attribute weights follows:

Attribute	Weight (0-100)
PC Fingerprint	80
Browser Fingerprint	50
IP Address	20
IP Geolocation	10
Browser Geolocation	40

Such a method may provide a proof of identity at the time of a transaction. In some exemplary embodiments, the method may be implemented in an embedded Java applet.

In some exemplary embodiments, the authentication system and/or method may provide payment integration with security features. Such embodiments may provide details and/or reports related to transactions, and may correlate security information with user data.

In some exemplary embodiments, an authentication system may provide fraud checks together with transaction data for a user. This may include a set of APIs that allow a merchant to plug in the payment instruments and/or accounts together with order information and/or payment information. Such a system may provide analytics about where users are from, which payment methods they typically use, among others.

In some exemplary embodiments, a dynamic set of checks may uniquely identify a user across network identities. A

network identity may be provided through the network signature. The network signature may be defined by the set of network attributes which may comprise the user's identity from the point of view of the merchant. For example, network attributes may include the IP addresses that the user has come from, the browser or computer information sampled in the application, and/or the cookie that indicates the same computer or browser has visited the Web site or merchant before.

In some exemplary embodiments, an authentication system may include a test to register the user to a new computer based on a required set of credentials. This may also bind the network signature to another computer and/or another network identity. In some exemplary embodiments, multiple payment methods may be accepted for the same network identity.

FIG. 4 illustrates an exemplary system 400 for assessing and authenticating a transaction, which may include a merchant computer system 402, a user computer system 404, and/or server system(s) 406, which may implement transaction assessment and authentication methods described herein. Server system(s) 406 may include an electronic signature scoring service 408, merchant electronic signature policies 410, anti-fraud systems and policies 412, and/or an external anti-fraud interface 414. Server system(s) 406 may be operatively connected to third party identity providers 416 and/or third party anti-fraud services 418. Merchant computer system 402 may include merchant code 420 (e.g., an electronic signature and fraud interface) and/or may be operatively connected to existing anti-fraud relations 422 and/or third party authentication services 424.

In some exemplary embodiments, the merchant computer system 402, user computer system 404, and/or server system(s) 406 may be in communication with each other directly or via network connections (such as the Internet, an intranet or other network). The user information (including network information, for example) may be transmitted to the user information database(s) for storage.

In some exemplary embodiments, an electronic commerce payment instrument verification system and/or method may use unique attributes of computers (e.g., such as is described in the cookie and network signature above) and/or prior purchasing behavior (e.g., such as the transaction list and transactions results that have been seen for the user) associated with a payment instrument to determine whether a person attempting to use the payment instrument is truly its owner. Some exemplary embodiments may include one or more servers configured to receive payment requests from merchant computer systems, where the servers and associated software may be configured to verify the identity of the payment instrument user prior to allowing the payment to be made to the merchant. For example, the servers may receive one or more pieces of information (which may be encrypted) from the user's computer to verify the location of the computer using the network address or other network characteristics. The servers may be configured to determine the degree to which the user's prior purchasing behavior correlates with the requested transaction. For example, the servers may compare the network address(es) used in the past to determine whether there is a correlation between the current transaction and the previous transaction(s). Based at least in part upon correlation and/or matching information between the previously collected data and the newly collected data, a transaction may be authorized.

Some exemplary embodiments may include a transaction assessment and authentication system that relies upon an

15

independent combination of an electronic signature and prior purchasing behavior to deny or allow use of a payment instrument in a transaction. For example, such a system may utilize one or more cookies on the user's computer in its assessment and authentication. Similarly, some exemplary methods may include evaluating a combination of an electronic signature (which may include one or more cookies) and prior purchasing behavior (e.g., such as the transactions attempts and the results returned by the payment processor or gateway) to deny or allow use of a payment instrument in a transaction.

To provide additional context for various aspects of the present invention, the following discussion is intended to provide a brief, general description of a suitable computing environment in which the various aspects of the invention may be implemented. While some exemplary embodiments of the invention relate to the general context of computer-executable instructions that may run on one or more computers, those skilled in the art will recognize that the invention also may be implemented in combination with other program modules and/or as a combination of hardware and software.

Generally, program modules include routines, programs, components, data structures, etc., that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that aspects of the inventive methods may be practiced with other computer system configurations, including single-processor or multi-processor computer systems, minicomputers, mainframe computers, as well as personal computers, hand-held wireless computing devices, microprocessor-based or program-mable consumer electronics, and the like, each of which can be operatively coupled to one or more associated devices. Aspects of the invention may also be practiced in distributed computing environments where certain tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

A computer may include a variety of computer readable media. Computer readable media may be any available media that can be accessed by the computer and includes both volatile and nonvolatile media, removable and non-removable media. By way of example, and not limitation, computer readable media may comprise computer storage media and communication media. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD ROM, digital video disk (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which may be used to store the desired information and which may be accessed by the computer.

An exemplary environment for implementing various aspects of the invention may include a computer that includes a processing unit, a system memory and a system bus. The system bus couples system components including, but not limited to, the system memory to the processing unit. The processing unit may be any of various commercially available processors. Dual microprocessors and other multi-processor architectures may also be employed as the processing unit.

16

The system bus may be any of several types of bus structure that may further interconnect to a memory bus (with or without a memory controller), a peripheral bus, and a local bus using any of a variety of commercially available bus architectures. The system memory may include read only memory (ROM) and/or random access memory (RAM). A basic input/output system (BIOS) is stored in a non-volatile memory such as ROM, EPROM, EEPROM, which BIOS contains the basic routines that help to transfer information between elements within the computer, such as during start-up. The RAM may also include a high-speed RAM such as static RAM for caching data.

The computer may further include an internal hard disk drive (HDD) (e.g., EIDE, SATA), which internal hard disk drive may also be configured for external use in a suitable chassis, a magnetic floppy disk drive (FDD), (e.g., to read from or write to a removable diskette) and an optical disk drive, (e.g., reading a CD-ROM disk or, to read from or write to other high capacity optical media such as the DVD). The hard disk drive, magnetic disk drive and optical disk drive may be connected to the system bus by a hard disk drive interface, a magnetic disk drive interface and an optical drive interface, respectively. The interface for external drive implementations includes at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies.

The drives and their associated computer-readable media provide nonvolatile storage of data, data structures, computer-executable instructions, and so forth. For the computer, the drives and media accommodate the storage of any data in a suitable digital format. Although the description of computer-readable media above refers to a HDD, a removable magnetic diskette, and a removable optical media such as a CD or DVD, it should be appreciated by those skilled in the art that other types of media which are readable by a computer, such as zip drives, magnetic cassettes, flash memory cards, cartridges, and the like, may also be used in the exemplary operating environment, and further, that any such media may contain computer-executable instructions for performing the methods of the invention.

A number of program modules may be stored in the drives and RAM, including an operating system, one or more application programs, other program modules and program data. All or portions of the operating system, applications, modules, and/or data may also be cached in the RAM. It is appreciated that the invention may be implemented with various commercially available operating systems or combinations of operating systems.

It is also within the scope of the disclosure that a user may enter commands and information into the computer through one or more wired/wireless input devices, for example, a touch-screen, a keyboard and a pointing device, such as a mouse. Other input devices may include a microphone (functioning in association with appropriate language processing/recognition software as known to those of ordinary skill in the technology), an IR remote control, a joystick, a game pad, a stylus pen, or the like. These and other input devices are often connected to the processing unit through an input device interface that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, an IEEE 1394 serial port, a game port, a USB port, an IR interface, etc.

A display monitor or other type of display device may also be connected to the system bus via an interface, such as a video adapter. In addition to the monitor, a computer may include other peripheral output devices, such as speakers, printers, etc.

17

The computer may operate in a networked environment using logical connections via wired and/or wireless communications to one or more remote computers. The remote computer(s) may be a workstation, a server computer, a router, a personal computer, a portable computer, a personal digital assistant, a cellular device, a microprocessor-based entertainment appliance, a peer device or other common network node, and may include many or all of the elements described relative to the computer. The logical connections depicted include wired/wireless connectivity to a local area network (LAN) and/or larger networks, for example, a wide area network (WAN). Such LAN and WAN networking environments are commonplace in offices, and companies, and facilitate enterprise-wide computer networks, such as intranets, all of which may connect to a global communications network such as the Internet.

The computer may be operable to communicate with any wireless devices or entities operatively disposed in wireless communication, e.g., a printer, scanner, desktop and/or portable computer, portable data assistant, communications satellite, any piece of equipment or location associated with a wirelessly detectable tag (e.g., a kiosk, news stand, restroom), and telephone. This includes at least Wi-Fi (such as IEEE 802.11x (a, b, g, n, etc.)) and Bluetooth™ wireless technologies. Thus, the communication may be a predefined structure as with a conventional network or simply an ad hoc communication between at least two devices.

The system may also include one or more server(s). The server(s) may also be hardware and/or software (e.g., threads, processes, computing devices). The servers may house threads to perform transformations by employing aspects of the invention, for example. One possible communication between a client and a server may be in the form of a data packet adapted to be transmitted between two or more computer processes. The data packet may include a cookie and/or associated contextual information, for example. The system may include a communication framework (e.g., a global communication network such as the Internet) that may be employed to facilitate communications between the client(s) and the server(s).

Some exemplary embodiments of the invention may accumulate results from transactions over time, such as charge backs and refunds. This information may help in assessing the fraud score of a transaction requested by the user. For example, a lower fraud score would result from knowledge that this user does regular charge backs, then merchants can apply their anti-fraud policy to determine whether the transaction would be accepted.

Some exemplary embodiments may be configured to associate a credit card or another payment instrument with more than one user, as in a family situation. Building a graph connecting multiple users to the devices, locations, and payment instruments may also affect the fraud score of a transaction. A graph may associate different entities through having common key attributes that may uniquely identify a user. For example, if two users share the same browser or PC fingerprint, then the graph may identify those two users as associated by sharing the browser or fingerprint. The same may apply for IP address, credit card number or billing address, for example.

In some exemplary embodiments, use of a payment instrument through a known trusted source (e.g., certain well-known and trusted online retailers) may establish a base reputation for a user with an electronic signature for a merchant or collection of merchants not affiliated with the trusted source. For example, recognizing the user's use of

18

the trusted source for a transaction may provide an increased level of confidence that the user is known to accurately to the service.

FIG. 5 is a block diagram illustrating an exemplary system 500 for assessing and authenticating transactions according to the present disclosure. One or more merchant computer systems 502, one or more user computer systems 504, and/or one or more server systems 506 may be operatively connected via one or more networks 508, such as the Internet, one or more intranets, etc. Server systems 506 may include a transaction authentication tool interface 510, which may be operatively connected to one or more transaction authentication tool management databases 512, one or more user information databases 514 (which may include user data, authentication data, transaction data, etc.), and/or transaction authentication tool software 516 (which may be provided on one or more computer-readable media 518).

FIG. 6 is a block diagram illustrating an exemplary computer-readable medium 600 including computer-executable instructions stored thereon, which, when executed by a computer, enable the computer to perform a method 602 including the following operations. Operation 604 may include storing a first electronic signature associated with a user, the first electronic signature including a plurality of attributes collected in connection with a prior transaction. Operation 606 may include associating the first electronic signature with a payment instrument utilized in the prior transaction. Operation 608 may include receiving a second electronic signature in connection with a proposed transaction utilizing the payment instrument. Operation 610 may include comparing the second electronic signature with the first electronic signature. Operation 612 may include, if the second electronic signature correlates with the first electronic signature, confirming that the payment instrument and the second electronic signature are associated with one another. Operation 614 may include, if the second electronic signature does not correlate with the first electronic signature, determining that the payment instrument and the second electronic signature are not associated with one another.

FIG. 7 is a block diagram illustrating an exemplary computer-readable medium 700 including computer-executable instructions stored thereon, which, when executed by a computer, enable the computer to perform a method 702 including the following operations. Operation 704 may include receiving a received electronic signature including a plurality of received attributes and information pertaining to a payment instrument. Operation 706 may include comparing the plurality of received attributes of the received electronic signature to a plurality of stored attributes associated with a plurality of stored electronic signatures. Operation 708 may include, if the received electronic signature correlates with one of the plurality of stored electronic signatures, determining whether the payment instrument is associated with the one of the plurality of stored electronic signatures based at least in part upon at least one prior transaction involving the one of the plurality of stored electronic signatures and the payment instrument and, if the payment instrument is associated with the one of the plurality of stored electronic signatures, confirming an association between the payment instrument and the received electronic signature. Operation 710 may include, if the received electronic signature does not correlate with one of the plurality of stored electronic signatures, determining that the payment instrument is not associated with the received electronic signature.

FIG. 8 is a block diagram illustrating an exemplary computer-readable medium 800 including computer-execut-

19

able instructions stored thereon, which, when executed by a computer, enable the computer to perform a method **802** including the following operations. Operation **804** may include receiving, from a user computer system, a request to utilize a payment instrument in a transaction. Operation **806** 5 may include transmitting, to an authentication system, information pertaining to the payment instrument and a collected electronic signature including attributes associated with the user computer system. Operation **808** may include receiving, from the authentication system, an indication of whether the collected electronic signature associated with the user com- 10 puter system correlates with a stored electronic signature associated with the payment instrument obtained in connection with a previous transaction involving the user computer system and the payment instrument. 15

While exemplary embodiments have been set forth above for the purpose of disclosure, modifications of the disclosed embodiments as well as other embodiments thereof may occur to those skilled in the art. Accordingly, it is to be understood that the disclosure is not limited to the above 20 precise embodiments and that changes may be made without departing from the scope. Likewise, it is to be understood that it is not necessary to meet any or all of the stated advantages or objects disclosed herein to fall within the scope of the disclosure, since inherent and/or unforeseen 25 advantages of the may exist even though they may not have been explicitly discussed herein.

What is claimed is:

1. An authentication system for electronic transactions 30 occurring over a computerized network, the system comprising:

a transaction authentication system interface operatively coupled to the computerized network for receiving proposed transaction information over the computer- 35 ized network;

a user information database; and

a transaction authentication tool, operatively coupled to the transaction authentication system interface and to the user information database and configured to per- 40 form the steps of:

receiving, from the transaction authentication system interface, a request to utilize a payment instrument in a transaction;

receiving, from the transaction authentication system 45 interface, information pertaining to the payment instrument, information pertaining to a user computer system used to initiate the transaction, and a collected electronic signature representation of a user including attributes associated with the user 50 computer system; and

determining, by the transaction authentication tool, an indication of (a) a match score between the collected electronic signature representation of the user asso- 55 ciated with the user computer system and an electronic signature stored in the user information database to establish a user identity, (b) whether the payment instrument matches a payment instrument stored in the user information database, (c) whether the user computer system matches a computer iden- 60 tification stored in the user information database, (d) whether the user identity, the user computer system and the payment instrument have been previously used together, and (e) whether the user identity, the user computer system and the payment instrument all 65 have transaction reputations of a predetermined category;

20

transmitting by the transaction authentication tool:

(w) an indication that the transaction be rejected if the transaction authentication tool determines that the at least one of the user identity, the user computer system and the payment instrument does not have transaction reputations of the predeter- 5 mined category,

(x) an indication that the transaction be subject to scrutiny of a first predetermined level if the authentication transaction tool determines that the match score is above a threshold,

the payment instrument matches a payment instru- ment stored in the user information database, the user computer system matches a computer 10 identification stored in the user information database,

the user identity, the user computer system and the payment instrument have been previously used together, and

the user identity, the user computer system and the payment instrument all have transaction repu- 15 tations of the predetermined category,

(y) an indication that the transaction be subject to scrutiny of the first predetermined level if the authentication transaction tool determines that the match score is below the threshold,

the payment instrument matches a payment instru- ment stored in the user information database, the user computer system matches a computer 20 identification stored in the user information database,

the user identity, the user computer system and the payment instrument have been previously used together, and

the user identity, the user computer system and the payment instrument all have transaction repu- 25 tations of the predetermined category, and

(z) an indication that the transaction be subject to scrutiny of a second predetermined level if none of (w), (x) and (y) are satisfied;

wherein electronic signatures collected and stored in the user information database include at least one of:

browser fingerprint attributes associated with an indi- vidual's browser, the browser fingerprint attributes including two or more attributes taken from the group consisting of:

(i) operating system identity,

(ii) screen resolution,

(iii) software plug-ins,

(iv) time zone,

(v) system language,

(vi) information pertaining to whether Java is enabled,

(vii) information pertaining to whether cookies are enabled,

(viii) information pertaining to sites visited by a user's computer, and

(ix) information pertaining to social network friends of a user; and

computer fingerprint attributes associated with an indi- vidual's computer, the computer fingerprint attri- butes including a plurality of attributes taken from the group consisting of:

(i) processor characteristics,

(ii) machine memory size,

(iii) values loaded at predetermined locations in the individual's computer,

21

(iv) values loaded into a registry in an operating system of the individual's computer,
 (v) Ethernet MAC address,
 (vi) network information,
 (vii) programs loaded onto the individual's computer, and
 (viii) log files in the individual's computer.

2. An authentication system for electronic transactions occurring over a computerized network, the system comprising:

- a transaction authentication system interface operatively coupled to the computerized network for receiving proposed transaction information and additional computer network information over the computerized network, the additional computer network information being collected by at least one of a computer cookie and an application programming interface stored on a computer initiating the proposed transaction information; at least one electronic storage device containing a user information database; and
- a transaction authentication tool, operatively coupled to the transaction authentication system interface and to the user information database and configured to perform the steps of:
 - storing a first electronic signature representation of a first user in the user information database, the first electronic signature including a plurality of attributes associated with the first user's identity collected in connection with a prior transaction associated with a first entity taken from the group consisting of a first merchant, a first bank and a first payment processor; associating the first electronic signature with a payment instrument utilized in the prior transaction;
 - receiving from the transaction authentication system interface a second electronic signature representation of a second user in connection with a proposed transaction utilizing a payment instrument, the second electronic signature including a plurality of attributes associated with the second user's identity collected in connection with the proposed transaction associated with a second entity, different than the first entity, taken from the group consisting of a second merchant, a second bank and a second payment processor;
 - determining whether the second electronic signature correlates with the first electronic signature by comparing the second electronic signature with the first electronic signature to determine the identity of the second user relative to the first user; and
 - determining whether the proposed transaction is authorized based upon establishing the identity of the second user relative to the first user;

wherein the plurality of attributes associated with the first user's identity and the plurality of attributes associated with the second user's identity include:

- browser fingerprint attributes associated with an individual's browser, the browser fingerprint attributes including two or more attributes taken from the group consisting of (i) operating system identity, (ii) screen resolution, (iii) software plug-ins, (iv) time zone, (v) system language, (vi) information pertaining to whether Java is enabled, (vii) information pertaining to whether cookies are enabled, (viii) information pertaining to sites visited by a user's computer, and (ix) information pertaining to social network friends of a user; and

22

computer fingerprint attributes associated with an individual's computer, the computer fingerprint attributes including two or more attributes taken from the group consisting of (i) processor characteristics, (ii) machine memory size, (iii) values loaded at predetermined locations in the individual's computer, (iv) values loaded into a registry in an operating system of the individual's computer, (v) Ethernet MAC address, (vi) network information, (vii) programs loaded onto the individual's computer, and (viii) log files in the individual's computer;

wherein comparing the second electronic signature with the first electronic signature includes comparing individual attributes collected in connection with the proposed transaction to corresponding ones of the plurality of attributes collected in connection with the prior transaction so as to determine whether or not the identity of the user represented by the first electronic signature is the same as that performing the proposed transaction;

wherein determining whether the second electronic signature correlates with the first electronic signature is based at least in part upon a trust score calculated using a weighted consideration of at least some of the plurality of attributes collected in connection with the prior transaction;

wherein the weighted consideration includes calculating the trust score based at least in part upon matching attributes, non-matching attributes, and attributes not compared;

wherein the trust score is calculated using the following equation:

$$\frac{(\text{matchWeight}^2 - (\text{missWeight} * 2) - \text{notInRequest}) * 1000}{\text{maxPossible}^2}$$

wherein

- matchWeight corresponds to a sum of weights of all the matching attributes,
- missWeight corresponds to a sum of weights of all the non-matching attributes,
- notInRequest corresponds to a sum of weights of all the attributes not compared, and
- maxPossible corresponds to a sum of the weights of all the matching attributes, non-matching attributes and attributes not compared.

3. An authentication system for electronic transactions occurring over a computerized network, the system comprising:

- a transaction authentication system interface operatively coupled to the computerized network for receiving proposed transaction information over the computerized network;
- a user information database; and
- a transaction authentication tool, operatively coupled to the transaction authentication system interface and to the user information database and configured to perform the steps of:
 - receiving a received electronic signature representation of a user from the transaction authentication system interface, the received electronic signature including a plurality of received attributes associated with a user's identity and associated with a first entity taken from the group consisting of a first merchant, a first bank and a first payment processor;
 - receiving information pertaining to a proposed transaction associated with the received electronic signature; and

23

determining whether the received electronic signature correlates with any of a plurality of electronic signatures stored in the user information database by comparing the plurality of received attributes of the received electronic signature to a plurality of stored attributes associated with the plurality of stored electronic signatures;

wherein at least one of the plurality of stored electronic signatures are associated with a second entity, different from the first entity, taken from the group consisting of a second merchant, a second bank and a second payment processor;

wherein the plurality of received attributes and the plurality of stored attributes include:

- browser fingerprint attributes associated with an individual's browser, the browser fingerprint attributes including two or more attributes taken from the group consisting of (i) operating system identity, (ii) screen resolution, (iii) software plug-ins, (iv) time zone, (v) system language, (vi) information pertaining to whether Java is enabled, (vii) information pertaining to cookies are enabled, (viii) information pertaining to sites visited by a user's computer, and (ix) information pertaining to social network friends of a user; and
- computer fingerprint attributes associated with an individual's computer, the computer fingerprint attributes including a plurality of attributes taken from the group consisting of (i) processor characteristics, (ii) machine memory size, (iii) values loaded at predetermined locations in the individual's computer, (iv) values loaded into a registry in an operating system of the individual's computer, (v) Ethernet MAC address, (vi) network information, (vii) programs loaded onto the individual's computer, and (viii) log files in the individual's computer;

wherein determining whether the received electronic signature correlates with any of the plurality of stored electronic signatures includes determining which ones of the plurality of received attributes match stored attributes associated with individual stored electronic signatures;

wherein determining whether the received electronic signature correlates with any of the plurality of stored electronic signatures includes calculating a trust score based at least in part upon which ones of the plurality of received attributes match stored attributes associated with individual stored electronic signatures;

wherein calculating the trust score includes applying different weights to different ones of the plurality of received attributes; and

wherein the trust score is calculated based upon (a) a sum of weights of received attributes that match stored attributes, (b) a sum of weights of received attributes not matching the stored attributes, and (c) a sum of the weights of received attributes matching and not matching the stored attributes.

4. The authentication system of claim 3, wherein the trust score is calculated based upon (a) a sum of all the weights of received attributes that match stored attributes, (b) a sum of all the weights of received attributes not matching the stored attributes, and (c) a sum of all the weights of received attributes matching and not matching the stored attributes.

5. An authentication system for electronic transactions occurring over a computerized network, the system comprising:

24

a transaction authentication system interface operatively coupled to the computerized network for receiving proposed transaction information over the computerized network;

a user information database; and

a transaction authentication tool, operatively coupled to the transaction authentication system interface and to the user information database and configured to perform the steps of:

- receiving a received electronic signature representation of a user from the transaction authentication system interface, the received electronic signature including a plurality of received attributes associated with a user's identity and associated with a first entity taken from the group consisting of a first merchant, a first bank and a first payment processor;
- receiving information pertaining to a proposed transaction associated with the received electronic signature; and
- determining whether the received electronic signature correlates with any of a plurality of electronic signatures stored in the user information database by comparing the plurality of received attributes of the received electronic signature to a plurality of stored attributes associated with the plurality of stored electronic signatures;

wherein at least one of the plurality of stored electronic signatures are associated with a second entity, different from the first entity, taken from the group consisting of a second merchant, a second bank and a second payment processor;

wherein the plurality of received attributes and the plurality of stored attributes include:

- browser fingerprint attributes associated with an individual's browser, the browser fingerprint attributes including two or more attributes taken from the group consisting of (i) operating system identity, (ii) screen resolution, (iii) software plug-ins, (iv) time zone, (v) system language, (vi) information pertaining to whether Java is enabled, (vii) information pertaining to whether cookies are enabled, (viii) information pertaining to sites visited by a user's computer, and (ix) information pertaining to social network friends of a user; and
- computer fingerprint attributes associated with an individual's computer, the computer fingerprint attributes including a plurality of attributes taken from the group consisting of (i) processor characteristics, (ii) machine memory size, (iii) values loaded at predetermined locations in the individual's computer, (iv) values loaded into a registry in an operating system of the individual's computer, (v) Ethernet MAC address, (vi) network information, (vii) programs loaded onto the individual's computer, and (viii) log files in the individual's computer;

wherein determining whether the received electronic signature correlates with any of the plurality of stored electronic signatures includes determining which ones of the plurality of received attributes match stored attributes associated with individual stored electronic signatures;

wherein determining whether the received electronic signature correlates with any of the plurality of stored electronic signatures includes calculating a trust score based at least in part upon which ones of the plurality of received attributes match stored attributes associated with individual stored electronic signatures;

25

wherein calculating the trust score includes applying different weights to different ones of the plurality of received attributes; and

wherein the trust score is calculated based upon

- a which is a sum of weights of received attributes that match stored attributes,
- b which is a sum of weights of received attributes not matching the stored attributes,
- c which is a sum of weights of received attributes not compared with stored attributes, and
- d which is a sum of the weights of received attributes matching, not matching and not compared with the stored attributes.

6. The authentication system of claim 5, wherein the trust score is calculated from the following equation:

$$(a^2 - (b*2) - c) * 1000 / d^2.$$

7. A method for authenticating an electronic transaction received at a transaction authentication system interface, the method comprising the steps of:

receiving, from a transaction authentication system interface, a request to utilize a payment instrument in a transaction;

receiving, from the transaction authentication system interface, information pertaining to the payment instrument, information pertaining to a user computer system used to initiate the transaction, and a collected electronic signature representation of a user including attributes associated with the user computer system;

determining an indication of (a) a match score between the collected electronic signature representation of the user associated with the user computer system and an electronic signature stored in the user information database to establish a user identity, (b) whether the payment instrument matches a payment instrument stored in the user information database, (c) whether the user computer system matches a computer identification stored in the user information database, (d) whether the user identity, the user computer system and the payment instrument have been previously used together, and (e) whether the user identity, the user computer system and the payment instrument all have transaction reputations of a predetermined category; and

transmitting:

(w) an indication that the transaction be rejected if it is determined that the at least one of the user identity, the user computer system and the payment instrument does not have transaction reputations of the predetermined category,

(x) an indication that the transaction be subject to scrutiny of a first predetermined level if it is determined that the match score is above a threshold, the payment instrument is known, and matches a payment instrument stored in the user information database,

the user computer system is known, matches a computer identification stored in the user information database,

26

the user identity, the user computer system and the payment instrument have been previously used together, and

the user identity, the user computer system and the payment instrument all have transaction reputations of the predetermined category,

(y) an indication that the transaction be subject to scrutiny of the first predetermined level if it is determined that

the match score is below the threshold,

the payment instrument matches a payment instrument stored in the user information database,

the user computer system is known, matches a computer identification stored in the user information database,

the user identity, the user computer system and the payment instrument have been previously used together, and

the user identity, the user computer system and the payment instrument all have transaction reputations of the predetermined category, and

(z) an indication that the transaction be subject to scrutiny of a second predetermined level if none of (w), (x) and (y) are satisfied;

wherein electronic signatures collected and stored in the user information database include at least one of:

browser fingerprint attributes associated with an individual's browser, where the browser fingerprint attributes include two or more attributes taken from the group consisting of:

(i) operating system identity,

(ii) screen resolution,

(iii) software plug-ins,

(iv) time zone,

(v) system language,

(vi) information pertaining to whether Java is enabled,

(vii) information pertaining to whether cookies are enabled,

(viii) information pertaining to sites visited by a user's computer, and

(ix) information pertaining to social network friends of a user; and

computer fingerprint attributes associated with an individual's computer, where the computer fingerprint attributes include a plurality of attributes taken from the group consisting of:

(i) processor characteristics,

(ii) machine memory size,

(iii) values loaded at predetermined locations in the individual's computer,

(iv) values loaded into a registry in an operating system of the individual's computer,

(v) Ethernet MAC address,

(vi) network information,

(vii) programs loaded onto the individual's computer, and

(viii) log files in the individual's computer.

* * * * *